ELSEVIER Linear Algebra and its Applications 346 (2002) 1–14

LINEAR ALGEBRA AND ITS APPLICATIONS

www.elsevier.com/locate/laa

An algorithmic version of the theorem by Latimer and MacDuffee for 2×2 integral matrices

A. Behn [a,*], A.B. Van der Merwe [b]

[a] *Department of Mathematics, Texas A&M University, College Station, TX 77843, USA*
[b] *Department of Mathematics, University of Stellenbosch, 7600 Stellenbosch, South Africa*

Received 18 December 2000; accepted 7 September 2001

Submitted by R.A. Brualdi

Abstract

Given two $n \times n$ integral matrices A and B, they are said to be equivalent if $B = S^{-1}AS$, where S is an $n \times n$ integral matrix with determinant ± 1. If we consider $n \times n$ integral matrices with a fixed characteristic polynomial that is irreducible over $\mathbb{Q}$, it is well known from a result by Latimer and MacDuffee that the number of matrix classes (equivalence classes of matrices) is equal to the number of ideal classes ($I \cong J$ if $I = qJ$ for some q in the quotient field) of the ring obtained by adjoining a root of the characteristic polynomial to $\mathbb{Z}$. In this paper, we develop an effective version of this result for 2×2 matrices. We present an algorithm which given a 2×2 matrix finds a canonical representative in its class. In particular this allows us to determine whether two matrices are equivalent.

1. Introduction

The matrix solutions of an algebraic equation $f(x) \equiv x^n + k_1 x^{n-1} + \cdots + k_n = 0$, with integral coefficients, that is irreducible over $\mathbb{Q}$, were studied by Latimer and MacDuffee in [6]. Denote by $\mathbb{M}_n(\mathbb{Z})$ all $n \times n$ matrices with integral coeficients, by $\mathrm{GL}_n(\mathbb{Z})$ all $n \times n$ matrices with integral coefficients and determinant ± 1, and by $\mathrm{SL}_n(\mathbb{Z})$ all $n \times n$ matrices with integral coefficients and determinant 1. If $A \in$

* Corresponding author. Tel.: +1-979-845-7803; fax: +1-979-845-6028.
E-mail addresses: abehn@math.tamu.edu (A. Behn), abvdm@land.sun.ac.za (A.B. Van der Merwe).

0024-3795/02/$ - see front matter
PII: S0024-3795(01)00518-3

$\mathbb{M}_n(\mathbb{Z})$, then all matrices of the class $S^{-1}AS$ will again be solutions if $S \in \mathrm{GL}_n(\mathbb{Z})$. In general, all solutions cannot be derived in this way from one solution only. The number of classes of matrix solutions coincides with the number of different classes of ideals in the ring $\mathbb{Z}[\alpha]$, where α is a root of the equation $f(x) \equiv x^n + k_1 x^{n-1} + \cdots + k_n = 0$. In [7, Chapter 3] it is stated that the general question of determining unique canonical forms with respect to this equivalence relation is unsolved.

Recent interest in this question has been spurred by results that link it to finding certain wavelet bases in $\mathbb{R}^2$. Bownik and Speegle [2] show that for any matrix in $\mathbb{M}_2(\mathbb{Z})$, there exists a (multi)-wavelet whose Fourier transform is compactly supported and smooth. A crucial part of their argument hinges on finding special representatives in the equivalence classes of integrally similar matrices.

We will consider the special case of matrices in $\mathbb{M}_2(\mathbb{Z})$, with a fixed characteristic polynomial $x^2 - \mathrm{tr}\, x + \det = 0$. For the most part we will assume that this polynomial is irreducible. So we have that the number of matrix classes is equal to the number of ideal classes of the ring $\mathbb{Z}[\alpha]$, where α is a root of the characteristic polynomial. In Section 2, we show how to set up a correspondence between matrix classes and classes of binary quadratic forms. In Sections 3 and 4, we will use known results and definitions from binary quadratic forms to define a reduced form for matrices in $\mathbb{M}_2(\mathbb{Z})$. In the case where the discriminant Δ of the characteristic polynomial is negative, we will have precisely one reduced matrix in each matrix class, and if $\Delta > 0$ and not a square in $\mathbb{Z}$, we will have a cycle of reduced matrices in each matrix class. We will use algorithms from binary quadratic forms, to obtain algorithms to reduce any integral matrix with a given characteristic polynomial, to a reduced matrix. Finally in Section 5, we deal with the case where the matrix has integral eigenvalues, that is the characteristic polynomial factors over the integers.

2. General results

Let us consider matrices in $\mathbb{M}_2(\mathbb{Z})$ with fixed trace (tr) and determinant (det). We associate with

$$M = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

the binary quadratic form

$$\phi(M) = \begin{bmatrix} -y & x \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = cx^2 + (d-a)xy - by^2$$

and with $(A, B, C) = Ax^2 + Bxy + Cy^2$ the matrix

$$\psi((A, B, C)) = \begin{bmatrix} \frac{\mathrm{tr}-B}{2} & -C \\ A & \frac{\mathrm{tr}+B}{2} \end{bmatrix}.$$

Notice that these maps are inverses of each other. Denote by Δ the discriminant of the characteristic polynomial of

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

Then $\Delta = \mathrm{tr}^2 - 4\det$, but it is also easy to verify that Δ is the discriminant of the binary quadratic form $cx^2 + (d-a)xy - by^2$. Thus under the above-mentioned association, the discriminant is preserved. Let $h \in \mathbb{Z}[x]$ be a fixed monic polynomial of discriminant Δ. We may consider ϕ as a map from matrices in $\mathbb{M}_2(\mathbb{Z})$ with characteristic polynomial h to binary quadratic forms of discriminant Δ, and ψ as a map from binary quadratic forms of discriminant Δ to matrices in $\mathbb{M}_2(\mathbb{Z})$ with characteristic polynomial h. Note that $\mathrm{tr} \equiv 1 \bmod 2$ if and only if $\Delta = \mathrm{tr}^2 - 4\det \equiv 1 \bmod 4$. But since Δ also equals $B^2 - 4AC$, this is equivalent to $B^2 - 4AC \equiv 1 \bmod 4$ or $B \equiv 1 \bmod 2$. Thus we conclude that

$$\begin{bmatrix} \frac{\mathrm{tr}-B}{2} & -C \\ A & \frac{\mathrm{tr}+B}{2} \end{bmatrix}$$

is in $\mathbb{M}_2(\mathbb{Z})$.

Definition 2.1. If $A, B \in \mathbb{M}_2(\mathbb{Z})$, then A and B are *equivalent* if there is a $C \in \mathrm{GL}_2(\mathbb{Z})$ such that $B = CAC^{-1}$.

The binary quadratic form $f(x, y) = Ax^2 + Bxy + Cy^2$ is equivalent to

$$f(\alpha x + \beta y, \gamma x + \delta y) = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}^{\mathrm{t}} \begin{bmatrix} A & B/2 \\ B/2 & C \end{bmatrix} \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix},$$

where

$$\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

In other words, (A, B, C) is equivalent to (A', B', C') if

$$\begin{bmatrix} A' & B'/2 \\ B'/2 & C' \end{bmatrix} = X^{\mathrm{t}} \begin{bmatrix} A & B/2 \\ B/2 & C \end{bmatrix} X$$

for some $X \in \mathrm{SL}_2(\mathbb{Z})$. We want to show that ϕ and ψ can be considered as maps between equivalence classes. To achieve this, we will enlarge our equivalence relation on binary quadratic forms. First we observe that if (A, B, C) and (A', B', C') are equivalent, then $(-A, B, -C)$ and $(-A', B', -C')$ are also equivalent. To see this, let

$$Y = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}$$

and let $Z = YXY \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\begin{aligned} Z^{\mathrm{t}} \begin{bmatrix} -A & B/2 \\ B/2 & -C \end{bmatrix} Z &= YX^{\mathrm{t}}Y \begin{bmatrix} -A & B/2 \\ B/2 & -C \end{bmatrix} YXY \\ &= YX \begin{bmatrix} -A & -B/2 \\ -B/2 & -C \end{bmatrix} XY \end{aligned}$$

$$= Y\begin{bmatrix} -A' & -B'/2 \\ -B'/2 & -C' \end{bmatrix} Y$$
$$= \begin{bmatrix} -A' & B'/2 \\ B'/2 & -C' \end{bmatrix}.$$

Thus we will also associate (A, B, C) with $(-A, B, -C)$.

Definition 2.2. (A, B, C) is *equivalent* to (A', B', C') if

$$\begin{bmatrix} A' & B'/2 \\ B'/2 & C' \end{bmatrix} = X^{\mathrm{t}} \begin{bmatrix} A & B/2 \\ B/2 & C \end{bmatrix} X$$

for some $X \in \mathrm{SL}_2(\mathbb{Z})$ and (A, B, C) is equivalent to $(-A, B, -C)$.

Next we show that ϕ and ψ may be considered as maps between classes. Direct calculations show that if $X \in \mathbb{M}_2(\mathbb{Z})$, $\phi(X) = f(x, y) = (A, B, C)$ and

$$Y = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

then

$$\phi(Y^{-1}XY) = f(\alpha x + \beta y, \gamma x + \delta y)$$

and

$$\phi\left(\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} X \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right) = (-A, B, -C).$$

Similarly,

$$\psi\big(f(\alpha x + \beta y, \gamma x + \delta y)\big) = Y^{-1}\psi(f(x, y))Y,$$

and

$$\psi(-A, B, -C) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \psi(A, B, C) \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

From the discussion in this section we have the following theorem.

Theorem 2.3. *The maps*

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = (c, d - a, -b) \quad \textit{and} \quad \psi(A, B, C) = \begin{bmatrix} \frac{\mathrm{tr} - B}{2} & -C \\ A & \frac{\mathrm{tr} + B}{2} \end{bmatrix}$$

are inverses of each other. They preserve the discriminant of the characteristic polynomial and binary quadratic form, as well as the equivalence relations as defined. More precisely, if $X \in \mathbb{M}_2(\mathbb{Z})$, $\phi(X) = f(x, y) = (A, B, C)$, *and*

$$Y = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

Table 1

Δ	$h(\Delta)$	Forms	Δ	$h(\Delta)$	Forms	Δ	$h(\Delta)$	Forms
-3	1	$(1, 1, 1)$	-12	1	$(1, 0, 3)$	-20	2	$(1, 0, 5)$
-4	1	$(1, 0, 1)$	-15	2	$(1, 1, 4)$			$(2, 2, 3)$
-7	1	$(1, 1, 2)$			$(2, 1, 2)$	-23	3	$(1, 1, 6)$
-8	1	$(1, 0, 2)$	-16	1	$(1, 0, 4)$			$(2, -1, 3)$
-11	1	$(1, 1, 3)$	-19	1	$(1, 0, 5)$			$(2, 1, 3)$

then

$$\phi(Y^{-1}XY) = f(\alpha x + \beta y, \gamma x + \delta y)$$

and

$$\phi\left(\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}X\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\right) = (-A, B, -C).$$

Similarly,

$$\psi\big(f(\alpha x + \beta y, \gamma x + \delta y)\big) = Y^{-1}\psi(f(x, y))Y$$

and

$$\psi(-A, B, -C) = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\psi(A, B, C)\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}.$$

3. $\Delta < 0$

First we recall some standard definitions on binary quadratic forms (see [1,3] or [4]).

Definition 3.1. A binary quadratic form (A, B, C), $(A, B, C \in \mathbb{Z})$ is *primitive* if $\gcd(A, B, C) = 1$, and *positive definite* if $A > 0$ and $\Delta = B^2 - 4AC < 0$. A positive definite binary quadratic form is *reduced* if $|B| \leqslant A \leqslant C$ and $B \geqslant 0$ if $|B| = A$ or $A = C$.

For $\Delta < 0$ we denote by $h(\Delta)$ (the class number of the discriminant) the number of primitive reduced binary quadratic forms with discriminant Δ.

For future examples and calculations we give a class number and primitive reduced binary quadratic forms for small discriminants as shown in Table 1.

Using Theorem 2.1 and Definition 3.1 it is clear how we should define reduced matrices if the discriminant of the characteristic polynomial is negative.

Definition 3.2. An integral matrix

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}$$

with $\Delta = \mathrm{tr}^2 - 4\det < 0$ is *reduced* if $|d-a| \leqslant c \leqslant -b$ and $d \geqslant a$ if $|d-a| = c$ or $c = -b$.

From the fact that we have exactly one reduced binary quadratic form in each equivalence class if $\Delta < 0$, we have from Theorem 2.1 the following result.

Theorem 3.3. *Consider matrices in* $\mathbb{M}_2(\mathbb{Z})$ *with a fixed* tr *and* det (*thus fixed characteristic polynomial*) *and with* $\Delta = \mathrm{tr}^2 - 4\det < 0$. *Then there is precisely one reduced matrix in each matrix class.*

How can we find all reduced matrices of a given trace and determinant?

1. Let $\Delta = \mathrm{tr}^2 - 4\det$ and determine all divisors Δ_i of Δ (in $\mathbb{Z}$) with $\Delta_i < 0$, $\Delta_i \equiv 0$ or $1 \bmod 4$ and $\Delta = \varepsilon_i^2 \Delta_i$ for some positive integer ε_i. Notice that to obtain reduced binary quadratic forms of discriminant Δ, we determine all primitive reduced quadratic forms (A, B, C) with discriminant Δ_i. Then $(\varepsilon_i A, \varepsilon_i B, \varepsilon_i C)$ have discriminant Δ.
2. With each primitive reduced quadratic forms (A, B, C) of discriminant Δ_i, we associate the reduced matrix
$$\psi(\varepsilon_i A, \varepsilon_i B, \varepsilon_i C) = \begin{bmatrix} \dfrac{\mathrm{tr} - \varepsilon_i B}{2} & -\varepsilon_i C \\ \varepsilon_i A & \dfrac{\mathrm{tr} + \varepsilon_i B}{2} \end{bmatrix}.$$
These $\sum h(\Delta_i)$ matrices will all be the reduced matrices of discriminant Δ.

Example 3.4. $\mathrm{tr} = 0,\ \det = 4,\ \Delta = -16 = 1(-16) = 2^2(-4)$
$$\psi(2x^2 + 2y^2) = \begin{bmatrix} 0 & -2 \\ 2 & 0 \end{bmatrix} \quad \text{and} \quad \psi(x^2 + 4y^2) = \begin{bmatrix} 0 & -4 \\ 1 & 0 \end{bmatrix}.$$
These are the only reduced matrices with $\mathrm{tr} = 0$ and $\det = 4$. Notice that we have two matrix classes with characteristic polynomial $x^2 + 4 = 0$, but the class number of $\mathbb{Z}[\sqrt{-4}]$ is 1. In terms of the theorem by Latimer and MacDuffee [6] this can be explained as follows. For this theorem to be true, we need to take the number of equivalence classes of ideals in $\mathbb{Z}[\alpha]$ (α is a root of the characteristic polynomial), where we define two ideals I and J to be equivalent if $I = qJ$ for some element q in the quotient field of $\mathbb{Z}[\alpha]$. This is of course not the same as the class number in general, since not all ideals of $\mathbb{Z}[\alpha]$ are invertible if $\mathbb{Z}[\alpha]$ is not a maximal order.

Given a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$**, how can we reduce it?**

We use Theorem 2.1 to translate a known algorithm for binary quadratic forms into an algorithm for $\mathbb{M}_2(\mathbb{Z})$.

1. If $c < 0$, replace $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ by

$$\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}=\begin{bmatrix}a & -b\\ -c & d\end{bmatrix}.$$

This corresponds to replacing $(c, d-a, -b)$ by $(-c, d-a, b)$ if $c<0$.

2. If $c>-b$, or $c=-b$ and $-c\leqslant d-a<0$ replace

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}$$

by

$$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix}=\begin{bmatrix}d & -c\\ -b & a\end{bmatrix}.$$

This corresponds to replacing $f(x, y)=cx^2+(d-a)xy-by^2$ by $f(-y, x)=-bx^2-(d-a)xy+cy^2$ if $c>-b$, or $c=-b$ and $-c\leqslant d-a<0$.

3. If

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix}$$

is not reduced, let $n\in\mathbb{Z}$ with

$$\frac{d-a}{2c}-\frac{1}{2}\leqslant n<\frac{d-a}{2c}+\frac{1}{2}\ \text{and replace}\ \begin{bmatrix}a & b\\ c & d\end{bmatrix}\ \text{by}$$

$$\begin{bmatrix}1 & n\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & b\\ c & d\end{bmatrix}\begin{bmatrix}1 & -n\\ 0 & 1\end{bmatrix}=\begin{bmatrix}a+nc & -na+b-n^2c+nd\\ c & -nc+d\end{bmatrix}.$$

This corresponds to replacing $f(x, y)=cx^2+(d-a)xy-by^2$ by $f(x-ny, y)$ if $f(x, y)$ is not reduced.

4. Repeat 2 and 3 until the matrix is reduced.

This reduction procedure can also be understood in terms of the action of $\mathrm{SL}_2(\mathbb{Z})$ (or more precisely $\mathrm{PSL}_2(\mathbb{Z})$) on the complex upper half plane $\mathbf{H}$, where the matrix

$$M=\begin{bmatrix}\alpha & \beta\\ \gamma & \delta\end{bmatrix}$$

corresponds to the mapping

$$z\mapsto\frac{\alpha z+\beta}{\gamma z+\delta}.$$

Recall that if we denote the real part of a complex number by $\mathscr{R}$, then the fundamental domain F of $\mathrm{SL}_2(\mathbb{Z})$ is $F=\{z\in\mathbf{H}:|z|>1, -1/2<\mathscr{R}(z)<1/2\}\cup\{z\in\mathbf{H}:|z|\geqslant 1, \mathscr{R}(z)=-1/2\}\cup\{z\in\mathbf{H}:|z|=1, \mathscr{R}(z)\leqslant 0\}$. It is customary to associate with (A, B, C) the complex number $\tau=(-B+\sqrt{\Delta})/2A$. Thus we will associate with

$$\begin{bmatrix}a & b\\ c & d\end{bmatrix},$$

where $c > 0$, the complex number $\tau = (a - d + \sqrt{\Delta})/2c$. We now repeatedly replace τ by $-1/\tau$ or by $\tau + n$ for some $n \in \mathbb{Z}$, until the complex number τ ends up in the fundamental domain. Replacing

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

by

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} d & -c \\ -b & a \end{bmatrix},$$

corresponds to replacing τ by $-1/\tau$. Also, replacing

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

by

$$\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a + nc & -na + b - n^2c + nd \\ c & -nc + d \end{bmatrix},$$

corresponds to replacing τ by $\tau + n$.

Example 3.5. In this example we reduce the matrix $\begin{bmatrix} -115 & -189 \\ 70 & 115 \end{bmatrix}$.

1. $\begin{bmatrix} -115 & -189 \\ 70 & 115 \end{bmatrix}$

2. $\begin{bmatrix} -115 & -189 \\ 70 & 115 \end{bmatrix}$

   $\tau = (-230 + 2\imath\sqrt{5})/140$

3. $\dfrac{d-a}{2c} - \dfrac{1}{2} = \dfrac{230}{140} - \dfrac{1}{2} \leqslant 2 < \dfrac{230}{140} + \dfrac{1}{2}$

   $\begin{bmatrix} a + 2c & -2a + b - 4c + 2d \\ c & -2c + d \end{bmatrix} = \begin{bmatrix} 25 & -9 \\ 70 & -25 \end{bmatrix}$

   $\tau + 2 = (50 + 2\imath\sqrt{5})/140$

2. $\begin{bmatrix} -25 & -70 \\ 9 & 25 \end{bmatrix}$

   $-1/\tau = (-50 + 2\imath\sqrt{5})/18$

3. $\dfrac{d-a}{2c} - \dfrac{1}{2} = \dfrac{50}{18} - \dfrac{1}{2} \leqslant 3 < \dfrac{50}{18} + \dfrac{1}{2}$

$$\begin{bmatrix} a+3c & -3a+b-9c+3d \\ c & -3c+d \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 9 & -2 \end{bmatrix}$$

$\tau + 3 = (4 + 2\imath\sqrt{5})/18$

2. $\begin{bmatrix} -2 & -9 \\ 1 & 2 \end{bmatrix}$

$-1/\tau = -2 + \imath\sqrt{5}$

3. $\dfrac{d-a}{2c} - \dfrac{1}{2} = \dfrac{3}{2} \leqslant 2 < \dfrac{d-a}{2c} + \dfrac{1}{2}$

$$\begin{bmatrix} a+2c & -2a+b-4c+2d \\ c & -2c+d \end{bmatrix} = \begin{bmatrix} 0 & -5 \\ 1 & 0 \end{bmatrix}$$

$\tau + 2 = \imath\sqrt{5}$.

4. $\Delta > 0$ and not a square in $\mathbb{Z}$

Definition 4.1. A quadratic form (A, B, C) with positive discriminant $\Delta = B^2 - 4AC$ (Δ not a square in $\mathbb{Z}$) is *reduced* if $|\sqrt{\Delta} - 2|A|| < B < \sqrt{\Delta}$.

It can be shown that if (A, B, C) is reduced, then $|A| + |C| < \sqrt{\Delta}$. Also, (A, B, C) is reduced if and only if $|\sqrt{\Delta} - 2|C|| < B < \sqrt{\Delta}$.

Definition 4.2. An integral matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

with $\Delta = \mathrm{tr}^2 - 4\det > 0$ and Δ not a square in $\mathbb{Z}$ is *reduced* if $c > 0$ and $|\sqrt{\Delta} - 2c| < (d-a) < \sqrt{\Delta}$.

If $A \neq 0$ and B are integers, we define $r(B, A)$ to be the unique integer such that $r \equiv B \bmod 2A$ and $-|A| < r \leqslant |A|$ if $|A| > \sqrt{\Delta}$, $\sqrt{\Delta} - 2|A| < r < \sqrt{\Delta}$ if $|A| < \sqrt{\Delta}$. In addition, we define the reduction operator ρ on (A, B, C) by

$$\rho(A, B, C) = \left(C, r(-B, C), \frac{r(-B, C)^2 - \Delta}{4C}\right).$$

In order to reduce (A, B, C), we apply ρ until the binary quadratic form is reduced. In general, there will not exist only one reduced form per equivalence class,

but several, which are organized in a cycle structure. If (A, B, C) is reduced, then $\rho(A, B, C)$ is again reduced, and the reduced forms equivalent to (A, B, C) are exactly $\rho^n(A, B, C)$ for n sufficiently large (i.e., n greater than or equal to the least n_0 such that $\rho^{n_0}(A, B, C)$ is reduced) and are finite in number. Recall that in order to calculate the class number $h(\Delta)$, we identify (A, B, C) and $(-A, B, -C)$. Notice that if $\rho(A, B, C) = (\alpha, \beta, \gamma)$, then $\rho(-A, B, -C) = (-\alpha, \beta, -\gamma)$. The class number $h(\Delta)$ equals the number of cycles of primitive reduced binary quadratic forms of discriminant Δ, where (A, B, C) and $(-A, B, -C)$ are identified.

Let $n = (-r(-B, C) - B)/2C$. Notice that from the definition of $r(-B, C)$ it follows that n is an integer. It is also easy to verify that applying ρ to (A, B, C) is equivalent to replacing $f(x, y) = Ax^2 + Bxy + Cy^2$ by $f(-y, x - ny)$.

Define the reduction operator P on the matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

as follows: if $-b > 0$,

$$P\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} -n & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & -n \end{bmatrix} = \begin{bmatrix} -nb + d & na + n^2b - c - nd \\ -b & a + nb \end{bmatrix},$$

where

$$n = \frac{r(a - d, b) + d - a}{2b}.$$

This is equivalent to replacing $f(x, y) = cx^2 + (d - a)xy - by^2$ by $f(-y, x - ny)$.

If $b > 0$, let

$$P\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} -n & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & n \end{bmatrix} = \begin{bmatrix} -nb + d & -na - n^2b + c + nd \\ b & a + nb \end{bmatrix},$$

where

$$n = \frac{r(a - d, b) + d - a}{2b}.$$

This is equivalent to replacing the $f(x, y) = cx^2 + (d - a)xy - by^2$ by $f(-y, x - ny) = cy^2 + (a - d)(x - ny)y - b(x - ny)^2$, and then replacing $cy^2 + (a - d)(x - ny)y - b(x - ny)^2$ by $-cy^2 + (a - d)(x - ny)y + b(x - ny)^2$.

Theorem 4.3. *Consider all matrices in* $\mathbb{M}_2(\mathbb{Z})$ *with a fixed* tr *and* det (*thus fixed characteristic polynomial*). *Let* $\Delta = \mathrm{tr}^2 - 4\det > 0$ *with* Δ *not a square in* $\mathbb{Z}$. *Then*

there is precisely one cycle of reduced matrices in each matrix class. Thus for each matrix class there is a matrix

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

in the class and a positive integer n such that

$$P^i\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \quad \text{for } 0 \leqslant i \leqslant n$$

are all the reduced matrices in the class and

$$P^{n+1}\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}.$$

How can we find all reduced matrices of a given trace and determinant?

1. Let $\Delta = \mathrm{tr}^2 - 4\det > 0$ (Δ not a square in $\mathbb{Z}$) and determine all divisors Δ_i of Δ (in $\mathbb{Z}$) with $\Delta_i > 0$, $\Delta_i \equiv 0$ or $1 \bmod 4$ and $\Delta = \varepsilon_i^2 \Delta_i$ for some positive integer ε_i.
2. With each primitive reduced binary quadratic form (A, B, C) with $A > 0$ and discriminant Δ_i, we associate the reduced matrix

$$\begin{bmatrix} \dfrac{\mathrm{tr} - \varepsilon_i B}{2} & -\varepsilon_i C \\ \varepsilon_i A & \dfrac{\mathrm{tr} + \varepsilon_i B}{2} \end{bmatrix}.$$

Cycles of primitive reduced binary quadratic forms will correspond to cycles of reduced matrices. There will be $\sum h(\Delta_i)$ cycles of reduced matrices of discriminant Δ.

Given a matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, how can we reduce it?

At some stage

$$P^n\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)$$

will become cyclic. This cycle will be a cycle of reduced matrices and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

is equivalent to each of the reduced matrices in the cycle.

Example 4.4. $\mathrm{tr} = 2$, $\det = -9$, $\Delta = 40$.

The primitive reduced quadratic forms of discriminant 40 are $(1, 6, -1)$, $(-1, 6, 1)$, $(2, 4, -3)$, $(-2, 4, 3)$, $(3, 2, -3)$, $(-3, 2, 3)$, $(3, 4, -2)$, $(-3, 4, 2)$. Recall that we identified (A, B, C) with $(-A, B, -C)$. Notice that $\rho(1, 6, -1) = (-1, 6, 1) \sim (1, 6, -1)$, $\rho(2, 4, -3) = (-3, 2, 3)$, $\rho(-3, 2, 3) = (3, 4, -2)$, $\rho(3, 4, -2) = (-2, 4, 3) \sim (2, 4, -3)$. Since we have two cycles, $h(40) = 2$.

Thus the two cycles of reduced matrices are

$$\begin{bmatrix} -2 & 1 \\ 1 & 4 \end{bmatrix}$$

and the cycle

$$\begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}, \begin{bmatrix} 0 & 3 \\ 3 & 2 \end{bmatrix}, \begin{bmatrix} -1 & 2 \\ 3 & 3 \end{bmatrix}.$$

Notice that

$$P\left(\begin{bmatrix} -2 & 1 \\ 1 & 4 \end{bmatrix}\right) = \begin{bmatrix} -2 & 1 \\ 1 & 4 \end{bmatrix}$$

and

$$P\left(\begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}\right) = \begin{bmatrix} 0 & 3 \\ 3 & 2 \end{bmatrix}, \quad P^2\left(\begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}\right) = \begin{bmatrix} -1 & 2 \\ 3 & 3 \end{bmatrix},$$

and finally

$$P^3\left(\begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}\right) = \begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}.$$

In order to illustrate the reduction algorithm, let us reduce the matrix

$$\begin{bmatrix} 1 & 5 \\ 2 & 1 \end{bmatrix}.$$

Since $n = (r(0,5) + 1 - 1)/(2.(5)) = 0$,

$$P\left(\begin{bmatrix} 1 & 5 \\ 2 & 1 \end{bmatrix}\right) = \begin{bmatrix} 1 & 2 \\ 5 & 1 \end{bmatrix}.$$

This time $n = (r(0,4) + 1 - 1)/(2.(2)) = 1$, thus

$$P\left(\begin{bmatrix} 1 & 2 \\ 5 & 1 \end{bmatrix}\right) = \begin{bmatrix} -1 & 3 \\ 2 & 3 \end{bmatrix}.$$

5. $\Delta = k^2, k \in \mathbb{Z}$

We now consider the case where the characteristic polynomial of the matrix factors over the integers. Let us fix the notation by saying $f(x) = (x - a)(x - d)$, where $a \geqslant d$.

Definition 5.1. If $a \neq d$, the matrix

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}$$

in $\mathbb{M}_2(\mathbb{Z})$ is *reduced* if $0 \leqslant b < a - d$. Also,

$$\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}$$

is *reduced* if $b \geqslant 0$. These are the only reduced matrices if $\Delta = k^2,\ k \in \mathbb{Z}$.

Theorem 5.2. *Let $M \in \mathbb{M}_2(\mathbb{Z})$, and assume that the characteristic polynomial of M factors over $\mathbb{Z}$. Then M is equivalent to a reduced matrix. Moreover, this class representative is unique thus no two different reduced matrices are equivalent.*

Proof. Let $f(x, y) = (x - a)(x - d)$ be the characteristic polynomial of M. Choose $\begin{bmatrix} x \\ y \end{bmatrix}$ to be an eigenvector for M with eigenvalue a and such that x, y are relatively prime integers. By Euclid's algorithm, there are integers z, w such that $xz - yw = 1$. Let

$$P = \begin{bmatrix} x & w \\ y & z \end{bmatrix}.$$

Since P has determinant 1, we know that M is equivalent to

$$\begin{bmatrix} a & b' \\ 0 & d \end{bmatrix} = P^{-1}MP.$$

Recall that

$$\begin{bmatrix} 1 & -n \\ 0 & 1 \end{bmatrix}\begin{bmatrix} a & b' \\ 0 & d \end{bmatrix}\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b' + n(a - d) \\ 0 & d \end{bmatrix},$$

so, if $a \neq d$, M is equivalent to

$$\begin{bmatrix} a & b \\ 0 & d \end{bmatrix},$$

where $0 \leqslant b < a - d$.

To show that this reduced form is unique, let us consider first the case when $a \neq d$. Suppose

$$\begin{bmatrix} a & b' \\ 0 & d \end{bmatrix} = P^{-1}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}P, \quad 0 \leqslant b, b' < a - d.$$

Then P is of the form

$$\begin{bmatrix} \pm 1 & n \\ 0 & \pm 1 \end{bmatrix},$$

so that $b - b'$ is divisible by $d - a$. Thus $b = b'$.

Finally when both eigenvalues are the same,

$$\begin{aligned} P^{-1}\begin{bmatrix} a & b \\ 0 & a \end{bmatrix}P &= P^{-1}\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}P + P^{-1}\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}P \\ &= \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} + P^{-1}\begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}P. \end{aligned}$$

It is easy to verify that if

$$P^{-1}\begin{bmatrix}0 & b\\ 0 & 0\end{bmatrix}P = \begin{bmatrix}0 & b'\\ 0 & 0\end{bmatrix},$$

then $b = \pm b'$. □

References

[1] W.W. Adams, L.J. Goldstein, Introduction to Number Theory, Prentice-Hall, Englewoods Cliffs, NJ, 1976.
[2] M. Bownik, D. Speegle, Meyer type wavelet bases in $\mathbb{R}^2$, preprint.
[3] H. Cohen, A Course in Computational Algebraic Number Theory, GTM 138, Springer, Berlin, 1993.
[4] R. Kumanduri, C. Romero, Number Theory with Computer Applications, Prentice-Hall, Englewoods Cliffs, NJ, 1998.
[5] J.C. Lagarias, Y. Wang, Haar bases for $L^2(\mathbb{R}^n)$ and algebraic number theory, J. Number Theory 57 (1996) 181–197.
[6] C.G. Latimer, C.C. MacDuffee, A correspondence between classes of ideals and classes of matrices, Ann. Math. 34 (1933) 313–316.
[7] M. Newman, Integral Matrices, Academic Press, New York, 1972.
[8] O. Taussky, On a theorem of Latimer and MacDuffee, Canad. J. Math. 1 (1949) 300–302.